JOURNAL OF COMPUTER AND SYSTEM SCIENCES 24, 180–196 (1982)

Quadratic Automata

JERRY GOLDMAN AND STEVEN HOMER

Department of Mathematical Sciences,
DePaul University, Chicago, Illinois 60614

Received February 28, 1981; revised September 21, 1981

In this paper the notion of a quadratic automaton transformation is defined and studied. The automata considered transform infinite input sequences of elements from a finite commutative ring with identity to infinite output sequences. Results extending the linear automaton transformation theory of A. Nerode are derived and two distinct approaches to machine realization arise depending upon whether 2 is invertible in the base ring or not. Such a naturally occurring quadratic map as the AND function of elementary switching theory is easily realized in this setting.

Finite state machines have played a significant role in many areas of computer science, from systems theory to formal grammars and complexity theory. In studying these automata the class of linear finite state machines has arisen in several contexts (see Hopcroft and Ullman [3]). They play an important part in coding theory (see Kohavi [4]), where linear codes have been extensively studied. In addition, in systems theory, linear as well as multilinear finite state machines have been seen to yield new approaches to properties of and ways to interconnect arbitrary finite state automata (see Mohler [5] and Porter [7]). The notion of linear automaton transformation first appeared in Nerode [6], where such transformations are characterized in terms of matrices and where the seminal notion of a minimal finite state machine is first discussed.

It is well known that a linear finite state automaton with finite input and output alphabet can be realized by a network with three basic components; adders, scalar multipliers, and unit delays. Such an elementary circuit component as an AND gate, whose outputs are the products of its inputs, is precluded. We determine in this paper a large class of such quadratic transformations which can be realized by finite automata.

We base our approach on the basic work of Nerode [6] and consider automata which transform infinite input sequences to infinite output sequences. In Section 1 the notion of a quadratic automaton transformation as well as some notation is introduced and the fundamental theorem of Nerode is presented, slightly restated in more current terminology. The second section contains a parallel theorem giving an algebraic representation of quadratic automaton transformations when 2 is invertible in R. Section 3 covers the AND machine over Z_2. In Section 4 we characterize the

0022-0000/82/020180–17$02.00/0

quadratic automaton transformations over Z_2 which can be realized by an automaton. The principal result of Section 5 is that every quadratic automaton transformation with $1/2 \in R$ can be realized by a finite state machine, a quadratic automaton.

All of our results are stated over finite commutative rings with identity. There is a basic bifurcation in the results depending upon whether the ring has the element $1/2$ in it or not. This split is particularly apparent when considering the fundamental quadratic machine we call the AND machine which is widely applied in the characteristic two case. Section 3 contains an explicit construction of the AND machine over Z_2 as well as a precise statement of the setting in which such a machine can be realized. Finally, the last section mentions some extensions and further directions which this work may take.

1. Notation and Preliminary Results

Before defining our notion of a quadratic automaton transformation, we must introduce notation for a basic theorem of Nerode. Let R be a finite commutative ring with identity. For N equal to the set of non-negative integers, form R^N, the Cartesian product of $\aleph_0$ copies of R with itself. Thus, R^N is the set of all functions $f\colon N \to R$. R^N is an R-algebra under the pointwise addition and multiplication given by $(f+g)(i) = f(i) + g(i)$ and $(fg)(i) = f(i) \cdot g(i)$, and the module operation rf, where $(rf)(i) = r \cdot f(i)$ for all $f, g \in R^N$, $r \in R$, and $i \in N$. A map $M\colon C \to D$ is *linear* if $M(rf+g) = r \cdot M(f) + M(g)$ for all $f, g \in C$, $r \in R$, for C and D subalgebras of R^N.

Let A and B be finite nonempty sets and form product sets A^N, B^N as above. We tailor the definition in [6] to current usage as follows. Define a map $M\colon A^N \to B^N$ to be an *automaton transformation* if there exists a finite set Q, maps $M_Q\colon Q \times A \to Q$, $M_B\colon Q \times A \to B$, and an element $\bar{q} \in Q$ such that for each $f \in A^N$ there is an $h \in Q^N$ satisfying $h(0) = \bar{q}$,

$$\begin{aligned} Mf(n) &= M_B(h(n), f(n)), \\ h(n+1) &= M_Q(h(n), f(n)). \end{aligned} \tag{1}$$

We say that the automaton $(Q, A, B, \bar{q}, M_Q, M_B)$ *realizes* M. Here A and B are the input and output alphabets, Q is the state set, M_Q is the next state function, M_B the current output function, and $\bar{q}$ the initial or start state.

Define a matrix $u_{ij}\colon N \times N \to R$ to be *eventually doubly periodic* if there exist positive integers N_1, N_2, p_1, p_2 such that

$$\begin{aligned} u_{ij} &= u_{i+p_1,j} \qquad \text{for all } i > N_1 \text{ and all } j, \\ u_{ij} &= u_{i,j+p_2} \qquad \text{for all } j > N_2 \text{ and all } i. \end{aligned} \tag{2}$$

We can now state Nerode's Theorem in our modified terminology.

THEOREM 1. *Let R be a finite commutative ring with identity. The map $M: R^N \to R^N$ is a linear automaton transformation if there exists a matrix $u_{ij}: N \times N \to R$ such that:*

(i) *for $f \in R^N$ and $n \geqslant 0$,*

$$Mf(n) = u_{n0}f(0) + u_{n-1,1}f(1) + \cdots + u_{0n}f(n)$$

and

(ii) *u_{ij} is eventually doubly periodic.*

Suppose M: $C \to D$, where C and D are R-subalgebras of R^N. We call M a *quadratic automaton transformation* if

$$M(rf) = r^2M(f) \qquad \text{for all} \quad f \in C, \quad r \in R, \tag{3}$$

and the map B defined by

$$B(f, g) = M(f + g) - M(f) - M(g) \tag{4}$$

is a linear automaton transformation in each of its arguments. That is, the map of $C \to D$ given by $f \to B(f, g)$ for each fixed g is a linear automaton transformation, while $g \to B(f, g)$ for fixed f is a linear automaton transformation as well. A *quadratic automaton* is a finite state automaton which realizes a quadratic automaton transformation.

Observe that the bilinear map B: $C \times C \to D$ is symmetric in the sense that $B(f, g) = B(g, f)$ and that $B(f, f) = M(2f) - 2M(f) = 4M(f) - 2M(f) = 2M(f)$. Thus, if $1/2 \in R$, we can recapture $M(f) = (1/2)\,B(f, f)$ from B, while if R has characteristic 2, $B(f, f) = 0$, the zero function.

Define R_0^N to be the R-subalgebra of R^N which consists of all $f: N \to R$ such hat $f(i) \neq 0$ for only finitely many i.

Consider the following example in characteristic 2. Set $R = Z_2$ (the integers modulo 2) and define $M: R_0^N \to R_0^N$ by $(Mf)(n) = 0$ for $n = 0$, $(Mf)(n) = f(n-1) \cdot f(n)$ for $n \geqslant 1$. It is easy to calculate the associated bilinear map using (4) to find that $B(f, g)(0) = 0$ and that $B(f, g)(n) = f(n-1)\,g(n) + f(n)\,g(n-1)$ for $n \geqslant 1$. It is clear that this M satisfies (3), that B is linear in each of its arguments, and it will follow as a special case of our Theorem 4 that M is a quadratic automaton transformation. The M of this example is particularly interesting because it can be viewed as a generalized AND map and an automaton which realizes M (introduced later) can be viewed as an AND machine. Indeed, since we are working over Z_2, if $f \in R_0^N$ with $f(i) = 1$ for $0 \leqslant i \leqslant n$ and $f(i) = 0$ elsewhere, then after an initial output of 0, we have $Mf(i) = 1$ for $1 \leqslant i \leqslant n$. Conversely, if $Mf(i) = 1$ for $1 \leqslant i \leqslant n$, then $f(i) = 1$ for $0 \leqslant i \leqslant n$. The AND machine over Z_2 will be explicitly constructed and studied in more detail in Section 3.

2. Quadratic Automaton Transformations with $1/2$ in R

In this section we diagonalize quadratic automaton transformations $M: R^N \to R^N$, where $1/2 \in R$. We establish a converse for the largest possible subalgebra of R^N.

We will need the following definitions for Theorem 2, as well as in the sequel. Denote the nth projection map of $R^N \to R$ by Π_n. So, $\Pi_n(f) = f(n)$, $n \in N$. Also, for each $i \in N$, define the functions $\delta_i: N \to R$ by $\delta_i(j) = \delta_{ij}$ (the Kronecker delta).

THEOREM 2. *Let R be a finite commutative ring with identity. If $1/2 \in R$ and $M: R^N \to R^N$ is a quadratic automaton transformation then there exists a matrix $u_{ij}: N \times N \to R$ such that*

(i) *for all $f \in R^N$ and $n \geqslant 0$,*

$$Mf(n) = u_{n0} f^2(0) + u_{n-1,1} f^2(1) + \cdots + u_{0n} f^2(n)$$

and

(ii) *u_{ij} is eventually doubly periodic.*

Proof. First, it will prove convenient to rename the matrix elements u_{ij} which occur in Nerode's Theorem. We define $w_{ij} = 0$ for $j > i$ and $w_{ij} = u_{i-j,j}$ for $j \leqslant i$. In this notation, the periodicity properties (2) become

$$\begin{aligned} w_{ij} &= w_{i+p_2, j+p_2} \quad \text{for all } j > N_2 \text{ and all } i, \\ w_{ij} &= w_{i+p_1, j} \quad \text{for all } i > N_1 \text{ and all } j. \end{aligned} \tag{5}$$

Endow R with the discrete topology: since R is finite it is compact. Therefore, by the Tychonoff Theorem, R^N is compact in the product topology, and so is $R^N \times R^N$. It is well known that R is a topological ring, thus the sum and product maps taking $R \times R \to R$ are continuous. Recall that the open sets $O(f; x_1, \ldots, x_n)$ form a basis for the space R^N, where $O(f; x_1, \ldots, x_n) = \{ g: N \to R \mid g(x_i) = f(x_i),\ i = 1, \ldots, n \}$, $f \in R^N$, and $\{x_1, \ldots, x_n\} \subset N$.

For fixed n and f, the map $L_{n,f}: R^N \to R$ defined by $L_{n,f}(g) = B(f, g)(n)$ is continuous [6], since B is a linear automaton transformation in its second argument and thus satisfies (1), where output values depend only on $0, 1, \ldots, n$. Applying Theorem 1, we have

$$B(f, g)(n) = \sum_{i=0}^{n} w_{ni}(f)\, g(i), \tag{6}$$

where the $w_{ni}(f)$ satisfy the periodicity properties (5). For exactly the reason above, the map $f \to B(f, g)(n)$ of $R^N \to R$ is continuous for each fixed g and n. In particular, for $g = \delta_i$, Eq. (6) implies $B(f, \delta_i)(n) = w_{ni}(f)$; therefore, for each fixed n and i, the function $w_{ni}: R^N \to R$ is continuous. Consequently, the map $T_n: R^N \times R^N \to R$, defined by $T_n(f, g) = B(f, g)(n)$, is continuous, since it is the composite of continuous maps

$R^N \times R^N \to R \times R$ under (w_{ni}, Π_i), followed by $R \times R \to R$ under product, followed by an application of associativity and continuity of sum on $R \times R \to R$.

Now B is symmetric, thus

$$T_n(f, g) = \sum_{i=0}^{n} w_{ni}(f)g(i) = T_n(g, f) = \sum_{i=0}^{n} w_{ni}(g)f(i)$$

or

$$\sum_{i=0}^{n} [w_{ni}(f)g(i) - w_{ni}(g)f(i)] = 0. \tag{7}$$

Set $g = \delta_s$ and $f = \delta_t$ in (7). Observe that $g(i) = \delta_s(i) = \delta_{si}$ and that $f(i) = \delta_t(i) = \delta_{ti}$. We conclude

$$w_{ns}(\delta_t) = 0, \qquad \text{whenever} \quad s \neq t. \tag{8}$$

Using (6) and the definition of T_n, (8) implies $T_n(\delta_t, g) = \sum_{i=0}^{n} w_{ni}(\delta_t)\, g(i) = w_{nt}(\delta_t)\, g(t)$. Just setting $g = \delta_s$ in this last formula, we find that $T_n(\delta_t, \delta_s) = w_{nt}(\delta_t)\, \delta_s(t) = w_{nt}(\delta_t)\, \delta_{st}$, or

$$\begin{aligned} T_n(\delta_t, \delta_s) &= w_{ns}(\delta_s) \qquad \text{for} \quad t = s \\ &= 0 \qquad\qquad\ \ \text{if} \quad t \neq s. \end{aligned} \tag{9}$$

Since T_n is continuous on compact $R^N \times R^N$ we can use the form of the neighborhoods to establish "uniformity" in the sense that there is an m, such that for any $f, g \in R^N$, there are finite sums,

$$\sum_{t=0}^{m} f(t)\, \delta_t \qquad \text{and} \qquad \sum_{s=0}^{m} g(s)\, \delta_s$$

such that

$$T_n(f, g) = T_n\left(\sum_{t=0}^{m} f(t)\, \delta_t, \sum_{s=0}^{m} g(s)\, \delta_s\right).$$

Bilinearity and (9) imply that

$$T_n(f, g) = \sum_{t,s} f(t)\, g(s)\, T_n(\delta_t, \delta_s) = \sum_{t=0}^{m} w_{nt}(\delta_t) f(t)\, g(t).$$

Now write $W_{nt} = w_{nt}(\delta_t)$ and use the lower triangularity of the w_{ij} in (6) to see that

$$T_n(f, g) = \sum_{t=0}^{n} W_{nt} f(t)\, g(t), \tag{10}$$

where the W_{ij} carry over the periodicity properties of the w_{ij} in (5). Equate $f = g$ in (10) to get $T_n(f, f) = \sum_{t=0}^{n} W_{nt} f^2(t)$. Translate notation from W_{ij} to new u_{ij}'s to complete the proof of Theorem 2 by finally using $1/2 \in R$ to obtain $M(f)(n) = (1/2) B(f, f)(n) = (1/2) T_n(f, f)$.

It is not possible to prove the converse of Theorem 2 for an M acting on all of R^N. Instead, we establish a partial converse for quadratic automaton transformations acting on the eventually periodic sequence space defined as follows. Define a sequence $f \in R^N$ to be *eventually periodic* if there exist positive integers N_1 and p such that for all $i \geqslant N_1$, $f(i) = f(i + p)$. We denote the class of eventually periodic sequences of R^N by E. It is not hard to show that E is an R-subalgebra of R^N which properly contains R_0^N. Note that we do not need $1/2 \in R$ in the next theorem.

THEOREM 3. *Let R be a finite commutative ring with identity. If $M: E \to R^N$ satisfies* (i) *and* (ii) *of Theorem* 2, *then M is a quadratic automaton transformation.*

Proof. We find it convenient to use coefficients w introduced in the proof of Theorem 2 rather than the u's. Observe that for $Mf(n) = \sum_{t=0}^{n} w_{nt} f^2(t)$, we can compute

$$\begin{aligned} M(f + g)(n) - Mf(n) - Mg(n) &= \sum_{t=0}^{n} w_{nt}[(f(t) + g(t))^2 - f^2(t) - g^2(t)] \\ &= 2 \sum_{t=0}^{n} w_{nt} f(t)\, g(t) = B(f, g)(n). \end{aligned}$$

Thus, B is linear in each argument. That B is a linear automaton transformation in each argument follows from the periodicity properties of $2w_{nt}$, f, g, and the fact that E is a subring together with Theorem 1. Therefore M is a quadratic automaton transformation, which proves Theorem 3.

3. THE AND MACHINE

In Section 1 the AND map over $R = Z_2$ was defined to be $M: R_0^N \to R_0^N$, where $(Mf)(0) = 0$ and $(Mf)(n) = f(n-1) \cdot f(n)$ for $n \geqslant 1$. As noted there the bilinear map $B(f, g)$: $R_0^N \times R_0^N \to R_0^N$ associated with M is, $B(f, g)(0) = 0$, $B(f, g)(n) = f(n-1) \cdot g(n) + f(n) \cdot g(n-1)$ for $n \geqslant 1$. This AND map is important in that it is the canonical example of a map which cannot be realized by a linear finite state automaton.

It is natural to ask if our map M can be extended to map $R^N \to R^N$ and still give rise to a quadratic automaton transformation. In fact we will see this is not the case but that the domain of M can be extended to the subring E of R^N. The following

theorem has as a consequence that E is the largest subring of R^N ro which M can be extended while remaining a quadratic automaton transformation.

THEOREM 4. *Let g be a fixed sequence in Z_2^N. Define $B_g: Z_2^N \to Z_2^N$ by $B_g(f) = B(f, g)$, where as above, $B(f, g)(n) = f(n-1) \cdot g(n) + f(n) \cdot g(n-1)$ for $n \geqslant 1$ and $B(f, g)(0) = 0$. There is a finite state automaton which has B_g as an output function iff g is eventually periodic.*

Proof. Assume B_g is the output function of a finite state automaton. Note that for any finite state machine if an input sequence is eventually periodic then the output sequence is eventually periodic as well. (This is noted in Nerode [6].) Hence in particular if f is the sequence 0, 1, 0, 1, 0, 1,... then $B_g(f) = (0, g(0), g(2), g(2), g(4), g(4), g(6), g(6),...)$ is eventually periodic. If f is 1, 0, 1, 0,..., then

$$B_g(f) = (0, g(1), g(3), g(3),...)$$

is eventually periodic. From these it follows that the sequences

$$0, g(0), g(2), g(4),..., \ ... \qquad \text{and} \qquad 0, g(1), g(3), g(5),...$$

are eventually periodic. But then so is g.

Now assume g is eventually periodic. We will explicitly describe a finite state automaton which realizes B_g. As g is eventually periodic there exist integers L and P such that for any $i \geqslant L$, $g(i) = g(i+P)$. We will create a machine S whose states are used to code two consecutive elements of the finite sequence $g(0), g(1),..., g(L+P)$ as well as one element from the input sequence f.

Precisely $S = (Q, \{0, 1\}, \{0, 1\}, q_0, \delta, \lambda)$ where we define

$$\begin{aligned}
Q &= \{q_0\} \cup \{q_t^k \mid k \in Z_2,\ 1 \leqslant t \leqslant L+P\},\\
\delta(q_0, j) &= q_1^j, \qquad j \in Z_2,\\
\delta(q_t^k, j) &= q_{t+1}^j, \qquad t = 1, 2,..., L+P-1,\\
\delta(q_{L+P}^k, j) &= q_{L+1}^j,\\
\lambda(q_0, j) &= 0, \qquad j \in Z_2,\\
\lambda(q_t^k, j) &= j \cdot g(t-1) + k \cdot g(t), \qquad \text{for} \quad t = 1, 2,..., L+P.
\end{aligned}$$

See Figure 1 for a state diagram of this machine. Now note that for an input sequence $f \in Z_2^N$ we have, by induction on i, and the standard extension of δ to $Q \times Z_2^*$ (where Z_2^* is the free monoid generated by Z_2 under concatenation):

$$\begin{aligned}
\lambda(q_0, f(0),..., f(i)) &= q_{i+1}^{f(i)} \qquad \text{if } i \leqslant L+P-1.\\
&= q_{L+h+1}^{f(i)} \qquad \text{if } i \geqslant L+P, \text{ and } i = L+Py+h, \text{ where } y \text{ is an integer, and } 0 \leqslant h \leqslant P-1.
\end{aligned}$$

So $\lambda(q_0, f(0)) = 0$. Further, if $n \leqslant L + P$,

$$\begin{aligned}
&\lambda(q_0, f(0), f(1),..., f(n)) \\
&\quad = \lambda(\delta(q_0, f(0),..., f(n-1), f(n)) \\
&\quad = \lambda(q_n^{f(n-1)}, f(n)) \\
&\quad = f(n)\, g(n-1) + f(n-1)\, g(n).
\end{aligned}$$

If $n > L + P$, $n - 1 \geqslant L + P$, say $n - 1 = L + Py + h$. Then

$$\begin{aligned}
&\lambda(q_0, f(0), f(1),..., f(n)) \\
&\quad = \lambda(\delta(q_0, f(0),..., f(n-1), f(n)) \\
&\quad = \lambda(q_{L+h+1}^{f(n-1)}, f(n)) \\
&\quad = f(n)\, g(h + L) + f(n-1) \cdot g(L + h + 1) \\
&\quad = f(n) \cdot g(L + Py + h) + f(n-1) \cdot g(L + Py + h + 1), \\
&\qquad \text{since } g \text{ is eventually periodic with period } P, \\
&\quad = f(n)\, g(n-1) + f(n-1) \cdot g(n).
\end{aligned}$$

Hence in either case S realizes B_g and Theorem 4 is proved.

Note 1. A similar theorem holds for any finite commutative ring with identity with corresponding changes necessitated for Fig. 1.

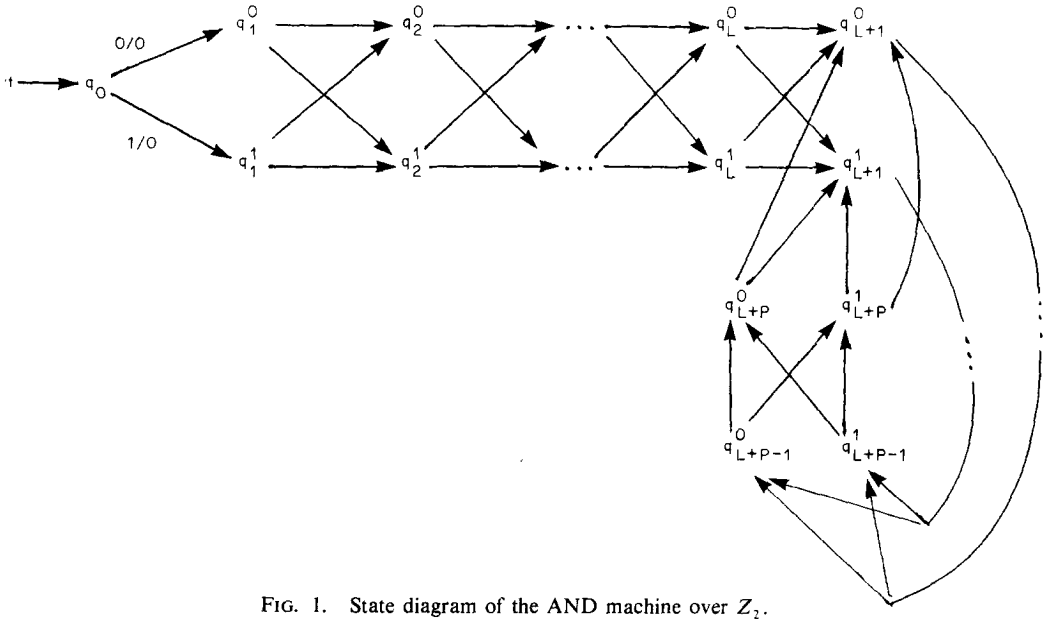

FIG. 1. State diagram of the AND machine over Z_2.

Note 2. One can show that B_g is translation invariant in the sense of Nerode [6]. A non-constructive proof of our Theorem 4 will then follow from a Corollary in that paper.

COROLLARY 5. *Let T be any subring of Z_2^N and define $M: T \to Z_2^N$ by $(Mf)(0) = 0$, $(Mf)(n) = f(n-1) \cdot f(n)$ for $n \geqslant 1$. Then M is a quadratic automaton transformation iff $T \subseteq E$.*

4. QUADRATIC AUTOMATON TRANSFORMATIONS OVER Z_2

In this section we give a representation and a partial characterization of quadratic automaton transformations over Z_2. The proof of the theorem here is quite long and technical. Much of the intuition for it comes from the AND machine of Section 3. First note that this case is very different from the case $1/2 \in R$ in that one cannot hope to prove that every quadratic automaton transformation can be realized by a quadratic automaton. For example, define $M: Z_2^N \to Z_2^N$ by $(Mf)(n) = f^2(n+1)$. Then $B(f, g)(n) = M(f+g)(n) - M(f)(n) - M(g)(n) = (f(n+1) + g(n+1))^2 - f^2(n+1) - g^2(n+1) = 0$; this B is trivially a linear automaton transformation in each variable. Consequently, M is a quadratic automaton transformation but clearly cannot be realized by any finite state machine since $Mf(n)$ is independent of $f(0),..., f(n)$.

So the question now turns to those quadratic automaton transformations which can be realized by finite automata. Before stating the theorem of this section we prove a general lemma concerning the output function of any finite state automaton over Z_2.

LEMMA 6. *Let $M: Z_2^N \to Z_2^N$ be an automaton transformation. Then M has the form $(Mf)(n) = \sum_T C_T^n(\prod_{i \in T} f(i))$, where the sum is taken over all subsets $T \subseteq \{0, 1,..., n\}$, $C_T^n \in Z_2$, and we interpret $\prod_{i \in \Phi} f(i) = 1$ when Φ is the empty set.*

Proof. For any finite set S, let $|S|$ denote the cardinality of S.

Fix an integer n. For any $S \subseteq \{0, 1,..., n\}$ define $\phi_S \in Z_2^N$, the characteristic function of S, by

$$\begin{aligned} \phi_S(k) &= 1 \qquad \text{if} \quad k \in S \\ &= 0 \qquad \text{otherwise,} \end{aligned}$$

and define $A_S^n = (M\phi_S)(n)$.

We now define C_S^n for any $S \subseteq \{0, 1,..., n\}$ by induction on $|S|$.

(i) $C_\Phi^n = A_\Phi^n$,

(ii) $C_S^n = A_S^n - \sum_{T \subsetneq S} C_T^n$, for any $S \neq \Phi$.

Now note that since M is an automaton transformation, the value of $(Mf)(n)$ depends only on $f(0), f(1),..., f(n)$. In particular, $(Mf)(n) = (M\phi_Q)(n)$ where $Q =$

$\{i \leqslant n \mid f(i) = 1\}$. We have $(M\phi_Q)(n) = A_Q^n = C_Q^n + \sum_{T \subsetneq Q} C_T^n$. Finally, use $\prod_{i \in T} \phi_Q(i) = 1$ iff $T \subseteq Q$ to see that

$$\begin{aligned}(Mf)(n) &= C_Q^n + \sum_{T \subsetneq Q} C_T^n = \sum_{T \subseteq Q} C_T^n \\ &= \sum_{T \subseteq \{0,1,\ldots,n\}} C_T^n \left(\prod_{i \in T} \phi_Q(i) \right) \\ &= \sum_{T \subseteq \{0,\ldots,n\}} C_T^n \left(\prod_{i \in T} f(i) \right).\end{aligned}$$

This completes the proof of Lemma 6.

The next concept plays the same role in the quadratic theory as eventually doubly periodic plays in the linear theory.

A sequence (C_{ij}^n) is defined to be *eventually triply periodic* iff

(i) $\exists N_1, p_1$ such that for $j \geqslant N_1$,

$$C_{k,j}^n = C_{k,j+p_1}^{n+p_1} \qquad \text{for any} \quad 0 \leqslant k < j \leqslant n.$$

(ii) $\exists N_2, p_2$ such that for any $j \geqslant N_2$,

$$C_{j,k}^n = C_{j+p_2,k}^{n+p_2} \qquad \text{for any} \quad j < k \leqslant n.$$

(iii) $\exists N_3, p_3$ such that for any j, k, n with $j \leqslant k \leqslant n$, if $n - k \geqslant N_3$ then

$$C_{j,k}^n = C_{j,k}^{n+p_3}.$$

(iv) $\exists N_4, p_4$ such that for any $j > N_4$, $n \geqslant j$,

$$C_{j,j}^n = C_{j+p_4,j+p_4}^{n+p_4}.$$

We can now state our theorem concerning quadratic automata over Z_2. Recall that E is the set of all eventually periodic sequences of Z_2^N.

THEOREM 7. (I) *Let $M: Z_2^N \to Z_2^N$ be a quadratic automaton transformation which is realized by a finite state machine. Then M is of the form*

$$(Mf)(n) = \sum_{i \leqslant j \leqslant n} C_{i,j}^n f(i) f(j), \tag{11}$$

where $(C_{i,j}^n)$ is eventually triply periodic.

(II) *If $M: E \to Z_2^N$ is defined by* (11), *then M is a quadratic automaton transformation. Moreover E is the largest subring of Z_2^N for which this is true.*

Proof of I. By Lemma 6 we know that $(Mf)(n) = \sum_{T \subseteq \{0,\ldots,n\}} C_T^n (\prod_{i \in T} f(i))$. As M is a quadratic automaton transformation, $C_\Phi^n = 0$ for all n.

Claim 1. For any Q such that $|Q| > 2$ and each n we have $C_Q^n = 0$.

Proof of Claim 1. We give a proof by induction on $|Q| \geqslant 3$. Define $B: Z_2^N X Z_2^N \to Z_2^N$ by $B(f, g) = M(f+g) - M(f) - M(g)$. As M is a quadratic automaton transformation B is bilinear. So for any fixed f, $B(f, g) = B_f(g)$ defines a linear map B_f on Z_2^N. Let $|Q| = 3$. Define $Q = \{q_1, q_2, q_3\}$ and $g_i = \delta_{q_i}$ for $i = 1, 2$. Set $g_3 = g_1 + g_2$ and note that $\phi_Q = \delta_{q_1} + \delta_{q_2} + \delta_{q_3}$. Using the definition of B, we have

$$\begin{aligned} B_{\phi_Q}(g_1)(n) = {} & C^n_{\{q_1,q_2\}} \phi_Q(q_2)\, g_1(q_1) + C^n_{\{q_1,q_3\}} \phi_Q(q_3)\, g_1(q_1) \\ & + C^n_Q\, g_1(q_1)\, \phi_Q(q_2)\, \phi_Q(q_3), \end{aligned}$$

since terms involving singleton subsets of Q subtract out under the bilinearization of M. Similarly,

$$\begin{aligned} B_{\phi_Q}(g_2)(n) = {} & C^n_{\{q_1,q_2\}} \phi_Q(q_1)\, g_2(q_2) + C^n_{\{q_2,q_3\}}\, g_2(q_2)\, \phi_Q(q_3) \\ & + C^n_Q \phi_Q(q_1)\, g_2(q_2)\, \phi_Q(q_3), \end{aligned}$$

and

$$\begin{aligned} B_{\phi_Q}(g_3)(n) = {} & C^n_{\{q_1,q_2\}} (\phi_Q(q_1)\, g_3(q_2) + \phi_Q(q_2)\, g_3(q_1)) \\ & + C^n_{\{q_1,q_3\}} \phi_Q(q_3)\, g_3(q_1) + C^n_{\{q_2,q_3\}} \phi_Q(q_3)\, g_3(q_2) \\ & + C^n_Q (\phi_Q(q_1)\, g_3(q_2)\, \phi_Q(q_3) \\ & + \phi_Q(q_2)\, g_3(q_1)\, \phi_Q(q_3) + g_3(q_1)\, g_3(q_2)\, \phi_Q(q_3)). \end{aligned}$$

It follows that

$$\begin{aligned} B_{\phi_Q}(g_1)(n) + B_{\phi_Q}(g_2)(n) &= B_{\phi_Q}(g_3)(n) - C^n_Q\, g_3(q_1)\, g_3(q_2)\, \phi_Q(q_3) \\ &= B_{\phi_Q}(g_3)(n) - C^n_Q. \end{aligned}$$

Since B_{ϕ_Q} is linear we must have $C^n_Q = 0$ in the case $|Q| = 3$. As induction hypothesis assume that for any Q, $2 < |Q| < k$, we know that $C^n_Q = 0$.

Now let $|Q| = k$. Say $Q = \{q_1, \ldots, q_k\}$. Now set $g_1(x) = 1$ iff $x = q_1$, $g_2(x) = 1$ iff $x = q_2$, and $g_3 = g_1 + g_2$. Then

$$\begin{aligned} B_{\phi_Q}(g_1)(n) &= A_1 + C^n_Q\, g_1(q_1)\, \phi_Q(q_2) \cdots \phi_Q(q_k), \\ B_{\phi_Q}(g_2)(n) &= A_2 + C^n_Q \phi_Q(q_1)\, g_2(q_2)\, \phi_Q(q_3) \cdots \phi_Q(q_k), \\ B_{\phi_Q}(g_3)(n) &= A_3 + C^n_Q (g_3(q_1)\, \phi_Q(q_2) \cdots \phi_Q(q_k) \\ &\quad + \phi_Q(q_1)\, g_3(q_2)\, \phi_Q(q_3) \cdots \phi_Q(q_k) \\ &\quad + g_3(q_1)\, g_3(q_2)\, \phi_Q(q_3) \cdots \phi_Q(q_k)), \end{aligned}$$

where the A_1, A_2, A_3 all consist of terms with coefficients C^n_Q where $2 \leqslant |Q| < k$. By hypothesis all such C^n_Q with $2 < |Q| < k$ are 0.

It is easy to see, as in the case $|Q| = 3$, that all of the terms with $|Q| \leqslant 2$ are such that $A_1 + A_2 = A_3$. Thus

$$\begin{aligned} B_{\phi_Q}(g_1)(n) + B_{\phi_Q}(g_2)(n) &= B_{\phi_Q}(g_3)(n) + C_Q^n\, g_3(q_1)\, g_3(q_2)\, \phi_Q(q_1) \cdots \phi_Q(q_k) \\ &= B_{\phi_Q}(g_3)(n) + C_Q^n. \end{aligned}$$

Hence, since B_{ϕ_Q} is linear and $g_1 + g_2 = g_3$, we have $C_Q^n = 0$, which proves Claim 1.

Now define $C_{i,j}^n$ by $C_{i,j}^n = C_{\{i,j\}}^n$ for $i \leqslant j \leqslant n$, where $\{i, i\}$ is another notation for $\{i\}$. Then $(Mf)(n) = \sum_{i \leqslant j \leqslant n} C_{i,j}^n f(i)\, f(j)$, where we have used the result of Claim 1 and the fact that $f^2(i) = f(i)$ over Z_2. We can now write

$$B(f, g)(n) = \sum_{i<j\leqslant n} C_{i,j}^n (f(i)\, g(j) + f(j)\, g(i)).$$

Now fix $j \leqslant n$ in this last expression for $B(f, g)(n) = B_f(g)(n)$ and note that the coefficient of $g(j)$ is

$$\sum_{0\leqslant k<j} C_{k,j}^n f(k) + \sum_{j<k\leqslant n} C_{j,k}^n f(k).$$

Now for any fixed f, by Theorem 1, since B_f is a linear automaton transformation,

$$B_f g(n) = d_{n0}^f\, g(0) + d_{n-1,1}^f\, g(1) + \cdots + d_{0n}^f\, g(n),$$

where $(d_{i,j}^f)$ is an eventually doubly periodic sequence. The coefficient of $g(j)$ here is $d_{n-j,j}^f$ which equals the expression for $g(j)$ displayed above and we conclude that

$$d_{i,j}^f = \sum_{0\leqslant k<j} C_{k,j}^{i+j} f(k) + \sum_{j<k\leqslant i+j} C_{j,k}^{i+j} f(k).$$

Now specialize $f = \delta_{k_0}$, and we have

$$\begin{aligned} d_{i,j}^f &= 0 && \text{if} \quad k_0 > i + j \quad \text{or} \quad k_0 = j \\ &= C_{k_0 j}^{i+j} && \text{if} \quad k_0 < j \\ &= C_{j k_0}^{i+j} && \text{if} \quad j < k_0 \leqslant i + j. \end{aligned}$$

As $(d_{i,j}^f)$ is doubly periodic we have $\exists N_1, p_1$ where if $i \geqslant N_1$, then $d_{i+p_1,j}^f = d_{i,j}^f$. So if $i > N_1$, then

$$C_{k_0,j}^{i+j} = C_{k_0,j}^{i+p_1+j} \qquad \text{if} \quad k_0 < j \leqslant i + j,$$

and

$$C_{j,k_0}^{i+j} = C_{j,k_0}^{i+p_1+j} \qquad \text{if} \quad j < k_0 \leqslant i + j.$$

From this it is easily seen that clause (iii) of the definition of eventually triply

periodic holds for $(C^n_{i,j})$ in the case $j < k \leqslant n$. As well, we see that $\exists N_2, p_2$ such that if $j \geqslant N_2$, then

$$d^f_{i,j} = d^f_{i,j+p_2}.$$

So if $j > N_2$, then

$$C^{i+j}_{k_0 j} = C^{i+j+p_2}_{k_0, j+p_2} \qquad \text{for} \quad 0 \leqslant k_0 < j \leqslant i+j$$

and

$$C^{i+j}_{j k_0} = C^{i+j+p_2}_{j+p_2, k_0} \qquad \text{for} \quad 0 \leqslant j < k_0 \leqslant i+j.$$

So $(C^n_{i,j})$ satisfy clauses (i) and (ii) of the definition of eventually triply periodic.

To finish the proof of the fact that $(C^n_{i,j})$ is eventually triply-periodic we have to deal with $(C^n_{j,j})$, $j \leqslant n$. Here the fact that M is a quadratic automaton transformation will not help us since, as we have seen, when M is linearized the terms $C_{ii} f^2(i)$ in M drop out. However, appealing to the fact that M is recognized by a finite state machine as well as the facts concerning $(C^n_{i,j})$ where $i < j$ enables us to establish the following claims.

Claim 2. $\exists N_3, p_3$ such that for any $n - j > N_3$, if $n \geqslant j$, then

$$C^n_{j,j} = C^{n+p_3}_{j,j}$$

Claim 3. $\exists N_4, p_4$ such that for any $j > N_4$, if $n \geqslant j$, then

$$C^n_{j,j} = C^{n+p_4}_{j+p_4, j+p_4}.$$

Proof of Claim 2. As a result of Claim 1, we have

$$(Mf)(n) = \sum_{i<j\leqslant n} C^n_{ij} f(i) f(j) + \sum_{j\leqslant n} C^n_{jj} f^2(j).$$

Fix an integer k_0 and define $f \in Z_2^N$ by

$$f(x) = 1 \qquad \text{if} \quad x \leqslant k_0$$
$$= 0 \qquad \text{if} \quad x > k_0.$$

So f is eventually periodic and for any $n > k_0$,

$$(Mf)(n) = \sum_{i<j\leqslant k_0} C^n_{ij} + \sum_{j\leqslant k_0} C^n_{jj}.$$

Now Mf is eventually periodic and by part (iii) of the definition of eventually triply-periodic we have $\sum_{i<j\leqslant k_0} C^n_{ij}$ is eventually periodic as a function of n. Thus, since the sum of a periodic and a non-periodic sequence is non-periodic, $\sum_{j\leqslant k_0} C^n_{jj}$ is eventually periodic as a function of n. But then by successively taking $k_0 = 0, 1, 2, \ldots$, we see that (C^n_{jj}) is eventually periodic as a function of n as well, which implies Claim 2.

Proof of Claim 3. Let g be the constant function 1 and represent Mg as in Claim 1. Then

$$(Mg)(n) = \sum_{i<j\leqslant n} C_{ij}^n + \sum_{j\leqslant n} C_{jj}^n$$

and again Mg is eventually periodic.

Now by part (i) of the definition of eventually triply periodic,

$$C_{ij}^n = C_{i,j+p_1}^{n+p_1}, \qquad \text{for } j \text{ sufficiently large.}$$

Thus for any fixed i_0, $\sum_{j\leqslant n} C_{i_0 j}^n$ is eventually periodic. But then $\sum_{i<j\leqslant n} C_{ij}^n$ is eventually periodic as a function of n and j. Hence so is $\sum_{j\leqslant n} C_{jj}^n$ and Claim 3 follows.

Claims 2 and 3 complete the proof that (C_{ij}^n) is an eventually triply periodic sequence, which finishes the proof of part I of the Theorem. We now turn to the partial converse, part II.

Proof of II. Assume M is such that $(Mf)(n) = \sum_{i\leqslant j\leqslant n} C_{ij}^n f(i) f(j)$, with (C_{ij}^n) eventually triply periodic. Then $B(f, g)(n) = \sum_{i<j\leqslant n} C_{ij}^n (f(i)\, g(j) + f(j)\, g(i))$ and B is clearly a bilinear map. Now fix $f_0 \in E$. Say for $x > N_5$, that $f_0(x) = f_0(x + p_5)$ for some p_5. Then

$$\begin{aligned} B(f_0, g)(n) = B_{f_0}(g)(n) &= \sum_{i<j\leqslant n} C_{ij}^n (f_0(i)\, g(j) + f_0(j)\, g(i)) \\ &= (C_{01}^n f_0(1) + C_{02}^n f_0(2) + \cdots + C_{0n}^n f_0(n))\, g(0) \\ &\quad + (C_{01}^n f_0(0) + C_{12}^n f_0(2) + C_{13}^n f_0(3) + \cdots + C_{1n}^n f_0(n))\, g(1) \\ &\quad + (C_{02}^n f_0(0) + C_{12}^n f_0(1) + C_{23}^n f_0(3) \\ &\quad + C_{24}^n f_0(4) + \cdots + C_{2n}^n f_0(n))\, g(2) + \cdots . \end{aligned}$$

For all $i, j \geqslant 0$, define

$$d_{ij} = \sum_{0\leqslant k<j} C_{kj}^{i+j} f_0(k) + \sum_{j<k\leqslant i+j} C_{jk}^{i+j} f_0(k).$$

Then it is easy to check that

$$B_{f_0}(g)(n) = d_{n0}\, g(0) + d_{n-1,1}\, g(1) + \cdots + d_{0n}\, g(n).$$

By Theorem 1, to show that B_{f_0} is a linear automaton transformation it is sufficient to show that (d_{ij}) is eventually doubly periodic.

Define

$$\begin{aligned} M_1 &= \max(N_3, N_5), \\ q_1 &= 2p_3 p_5 M_1, \\ M_2 &= \max(N_1, N_2, N_3, N_5), \\ q_2 &= 2p_1 p_2 p_3 p_5 M_2. \end{aligned}$$

Then we claim that the following two relations hold:

(a) $d_{i+q_1,j} = d_{ij}$ for all $i > M_1$,

(b) $d_{i,j+q_2} = d_{ij}$ for all $j > M_2$.

We prove (b), which is the more difficult of the two facts. Let $j > M_2$, then

$$\begin{aligned} d_{i,j+q_2} &= \sum_{0 \leqslant k < j+q_2} C_{k,j+q_2}^{i+j+q_2} f_0(k) + \sum_{j+q_2 < k \leqslant i+j+q_2} C_{j+q_2,k}^{i+j+q_2} f_0(k) \\ &= \sum_{0 \leqslant k < j} C_{k,j+q_2}^{i+j+q_2} f_0(k) + \sum_{j \leqslant k < j+q_2} C_{k,j+q_2}^{i+j+q_2} f_0(k) \\ &\quad + \sum_{j < k \leqslant i+j} C_{j+q_2,k+q_2}^{i+j+q_2} f_0(k+q_2). \end{aligned} \tag{12}$$

Now the first of the sums on the right side of (12) becomes

$$\sum_{0 \leqslant k < j} C_{k,j+q_2}^{i+j+q_2} f_0(k) = \sum_{0 \leqslant k < j} C_{kj}^{i+j} f_0(k) \qquad \text{since } p_1 \mid q_2 \text{ and } j \geqslant N_1.$$

The second sum on the right side of (12) vanishes because

$$\sum_{j \leqslant k < j+q_2} C_{k,j+q_2}^{i+j+q_2} f_0(k) = 2 \sum_{j \leqslant k < j+q_2/2} C_{k,j+q_2/2}^{i+j+q_2/2} f_0(k) = 0,$$

since $j > N_5$, N_1, $p_5 \mid q_2/2$, $p_1 \mid q_2/2$, and we are working in Z_2. The last sum of (12) becomes

$$\begin{aligned} &\sum_{j < k \leqslant i+j} C_{j+q_2,k+q_2}^{i+j+q_2} f_0(k+q_2) \\ &\quad = \sum_{j < k \leqslant i+j} C_{j+q_2,k+q_2}^{i+j+q_2} f_0(k) && \text{since } j > N_5 \text{ and } p_5 \mid q_2, \\ &\quad = \sum_{j < k \leqslant i+j} C_{j+q_2,k+2q_2}^{i+j+2q_2} f_0(k) && \text{since } j > N_2,\ p_2 \mid q_2 \text{ from} \\ &&& \text{part (ii) of the definition} \\ &&& \text{of eventually triply periodic,} \\ &\quad = \sum_{j < k \leqslant i+j} C_{j+q_2,k+2q_2}^{i+j+3q_2} f_0(k) && \text{since } q_2 > N_3 \text{ and } p_3 \mid q_2 \text{ from} \\ &&& \text{part (iii),} \\ &\quad = \sum_{j < k \leqslant i+j} C_{jk}^{i+j} f_0(k) && \text{since } j > N_1,\ N_2,\ p_1 \mid q_2,\ p_2 \mid q_2, \\ &&& \text{from parts (i) and (ii).} \end{aligned}$$

Hence $d_{i,j+q_2} = \sum_{0 \leqslant k < j} C_{kj}^{i+j} f_0(k) + \sum_{j < k \leqslant i+j} C_{jk}^{i+j} f_0(k) = d_{ij}$, which proves (b) above.

We have thus shown that B_{f_0} is a linear automaton transformation for any $f_0 \in E$. Similarly, for $g_0 \in E$, one can show that $f \to B(f, g_0)$ is a linear automaton transformation. The fact that E is the largest subring of Z_2^N satisfying part II follows from

Theorem 4 of Section 3. We have now proved part II and the proof of Theorem 7 is complete.

5. Quadratic Automata

The construction in Theorem 4 shows directly that the AND map M is a quadratic automaton transformation. There is a simple quadratic automaton which realizes M. Over Z_2 its state diagram is given below as Fig. 2. The extension of all this to general R is clear.

The next theorem justifies our definition of quadratic automaton transformation in case $1/2 \in R$ by showing every quadratic automaton transformation is realized by a quadratic automaton.

We do this by appealing to a general methodology for state-space description given in terms of an abstract notion of Hankel matrix due to Arbib and Manes [1, 2]. Because of space limitations in this paper, reference is made to [2] for complete definitions and the realization theory of Hankel matrices.

Theorem 8. *Let R be a finite commutative ring with identity in which 2 is invertible. If $M: R^N \to R^N$ is a quadratic automaton transformation, then there is an essentially unique automaton $(Q, R, R, \bar{q}, M_Q, M_R)$ with minimal state set Q which realizes M.*

Proof. Being given a quadratic automaton transformation $M: R^N \to R^N$ is equivalent to being given all input/output maps $\Pi_n \circ M$ for $n \in N$. By Theorem 2, the response of $\Pi_n \circ M$ to an input sequence f is $\Pi_n \circ M(f) = (Mf)(n) = u_{n0} f^2(0) + u_{n-1,1} f^2(1) + \cdots + u_{0n} f^2(n)$, which depends only upon the first $n+1$ components of f. Thus, the general realization theory of Arbib and Manes will apply here since we will observe that M is given by a Hankel matrix H which, as well, satisfies certain recurrence conditions.

In fact, let the infinite matrix $H = (w_{ij})$, where $w_{ij} = 0$ for $j > i$ and $w_{ij} = u_{i-j,j}$ for $j \leqslant i$ for elements u_{ij} of Theorem 2. If we consider each matrix element as a left multiplication map then each element of H is an R-linear map. Consequently, H is a Hankel matrix. Moreover, the second of the periodicity properties (5) implies that H is column recurrent in the sense of [2]. The finiteness of R here guarantees the existence and uniqueness of the realization asserted in Theorem 8 up to isomorphism.

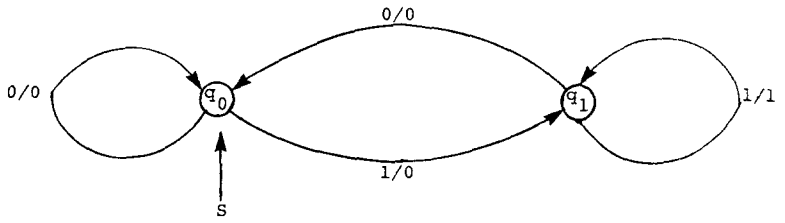

Figure 2

6. Final Remarks and Extensions

We conclude by mentioning an open problem and some further directions for research. Similar concepts could be defined and results stated for higher degree maps and automata. The proofs would be, for the most part, straightforward generalizations of those given here.

We did not define a quadratic automaton transformation M in terms of an initially given symmetric bilinear map $B: R^N \times R^N \to R^N$ using the definition $Mf = B(f, f)$ because then our AND map would not be a quadratic automaton transformation in characteristic = 2. Indeed, if $Mf(n) = f(n-1) \cdot f(n)$, then $M(f+g) - M(f) - M(g) = f(n-1)\ g(n) + g(n-1) f(n)$ which implies $B(f, f) = 2M(f) = 0$. Thus, there does not exist a bilinear map which can be used to define this M in characteristic 2. In the case that $1/2 \in R$, our definition is equivalent to the one above; however, in this case it would make more sense to generalize slightly with the affine definition $Mf = B(f, f) + L(f)$ for initially given bilinear and linear maps B and L. This would extract a greater gain for the price of losing the ability to call AND a quadratic automaton transformation in case 2 is not invertible in R.

It is an open question whether these results can be extended to an arbitrary commutative ring of characteristic two. Our results depend heavily upon properties of Z_2.

There are a number of possible interesting applications of quadratic automata. Chief among them are applications to coding theory [8] and to circuit theory.

References

1. M. A. Arbib and E. G. Manes, Generalized Hankel matrices and system realization, *SIAM J. Math. Anal.* **11** (1980), 405–424.
2. M. A. Arbib and E. G. Manes, Foundations of system theory: The Hankel matrix, *J. Comput. System Sci.* **20** (1980), 330–378.
3. J. Hopcroft and J. Ullman, "Introduction to Automata Theory, Languages and Computation," Addison–Wesley, Reading, Mass., 1979.
4. Z. Kohavi, "Switching and Finite Automata Theory," Second Ed., McGraw–Hill, New York, 1978.
5. R. R. Mohler, "Bilinear Control Processes," Academic Press, New York, 1973.
6. A. Nerode, Linear automaton transformations, *Proc. Amer. Math. Soc.* **9** (1958), 541–544.
7. W. A. Porter, Continuous state models for finite state machines, *Internat. J. Control* **25** (1977), 165–183.
8. J. E. Roos, An algebraic study of group and nongroup error-correcting codes, *Inform. Contr.* **8** (1965), 195–214.